ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, DAN BARNYARD2 PADA VPS UBUNTU

Skripsi

Disusun sebagai salah satu syarat menyelesaikan jenjang Strata 1

Pada Program Studi Informatika Fakultas Komunikasi dan Informatika

Universitas Muhammadiyah Surakarta

Oleh :

Alim Nuryanto

L200110022

PROGRAM STUDI INFORMATIKA

FAKULTAS KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS MUHAMMADIYAH SURAKARTA

2015

ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, DAN BARNYARD2 PADA VPS UBUNTU

Skripsi

Disusun sebagai salah satu syarat menyelesaikan jenjang Strata 1

Pada Program Studi Informatika Fakultas Komunikasi dan Informatika

Universitas Muhammadiyah Surakarta

Oleh :

Alim Nuryanto

L200110022

PROGRAM STUDI INFORMATIKA

FAKULTAS KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS MUHAMMADIYAH SURAKARTA

2015

HALAMAN PERSETUJUAN USULAN PENELITIAN

Skripsi dengan judul

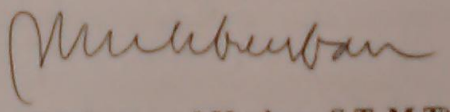
ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, BARNYARD2 PADA VPS UBUNTU

Telah disetujui pada :

Hari : Jum'at

Tanggal : 24 Juli 2015

Pembimbing 1



(Muhammad Kusban, S.T, M.T)

NIK : 663

SKRIPSI

ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, BARNYARD2 PADA VPS UBUNTU

Dipersiapkan dan disusun oleh :

Alim Nuryanto

L200110022

Pada tanggal 30 Juli 2015

Susunan Dewan Penguji

Pembimbing I

Muhammad Kusban, S.T, M.T

NIK. 663

Dewan Penguji I

Agus Ulinuha, S.T, M.T, Ph.D

NIK : 656

Dewan Penguji II

Dr. Heru Supriyono, M.Sc

NIK : 970

Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar sarjana

Tanggal 7 Agustus 2015

Dekan

Fakultas Komunikasi Informatika

Husni Thamrin, S.T., M.T., Ph.D.

NIK. 706

Ketua Program Studi

Informatika

Dr. Heru Supriyono, M.Sc.

NIK. 970

KONTRIBUSI

Dengan ini, peneliti menyatakan dengan sebenarnya bahwa Karya ini murni hasil dari penelitian sendiri dan sepengetahuan peneliti tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah dan disebutkan dalam daftar pustaka.

Berikut saya sampaikan daftar kontribusi dalam menyusun skripsi :

1. Peneliti melakukan penelitian aplikasi ini sendiri dengan bantuan buku, dan internet.
2. Software yang peneliti gunakan dalam pembuatan aplikasi adalah Suricata, Snorby, dan Barnyard2 dengan perangkat komputer pribadi.
3. Sistem operasi yang digunakan dalam penelitian adalah windows 7 64-bit dan Ubuntu LTS 12.04.

Apabila ternyata kelak ditemukan hari terbuktinya ada ketidakbenaran dalam pernyataan maka peneliti akan sepenuhnya bertanggungjawab sepenuhnya.

Surakarta, 2 Agustus 2015

Mengetahui

Pembimbing Tugas Akhir ,

Muhammad Kusban, S.T, M.T

NIK : 663

Penulis

Alim Nuryanto

NIM : L200110022

HALAMAN PERSEMBAHAN

Puji syukur peneliti panjatkan kehadirat Allah SWT, yang telah memberikan kesempatan kepada peneliti untuk menyelesaikan skripsi dengan judul "Analisis dan Implementasi Suricata, Snorby, dan Barnyard2 pada VPS Ubuntu". Shalawat serta salam peneliti panjatkan kepada Nabi besar Muhammad SAW karena beliaulah yang telah memimpin Umat Islam dari jaman kebodohan ke jaman penuh pengetahuan. Peneliti mempersembahkan karya ini kepada :

1. Kedua orang peneliti Sumaryono dan Setiani yang telah memberikan dukungan penuh kepada peneliti untuk menyelesaikan skripisi ini,
2. Muhammad Kusban, S.T, M.T yang telah membimbing peneliti dalam pengerjaan skripsi ini,
3. Teman - teman seangkatan ataupun beda angkatan yang menimba ilmu di Universita Muhammadiyah Surakarta yang tidak dapat peneliti sebutkan namanya satu - persatu.

Peneliti menyadari bahwa banyak kekurangan dari penyusunan skripsi ini. Namun, peneliti berharap skripsi ini dapat membantu menjadi referensi ataupun sebagai salah informasi yang dapat dimanfaatkan dengan baik oleh para pembaca.

KATA PENGANTAR

Puji syukur peneliti panjatkan kehadirat Allah SWT, yang telah menciptakan langit dan Bumi beserta isinya serta melimpahkan berbagai macam ilmu pengetahuan yang tidak terhitung jumlahnya. Shalawat serta salam peneliti panjatkan kepada Nabi besar Muhammad SAW karena beliaulah yang telah memimpin Umat Islam dari jaman kebodohan ke jaman penuh pengetahuan.

Skripsi dengan judul "Analisis dan Implementasi Suricata, Snorby, dan Barnyard2 pada VPS Ubuntu" disusun sebagai salah satu persyaratan akhir untuk mendapatkan gelar Sarjana di Universitas Muhammadiyah Surakarta pada Fakultas Komunikasi dan Informatika. peneliti mengucapkan terimakasih kepada :

1. Bapak Husni Tamrin, S.T, M.T selaku Dekan Fakultas Informatika Universitas Muhammadiyah Surakarta yang telah menandatangani halaman pengesahan makalah skripsi ini,
2. Bapak Dr. Heru Supriyono, S.T, M.T selaku Ketua Prodi Jurusan Informatika Universitas Muhammadiyah Surakarta yang telah menandatangani halaman pengesahan makalah skripsi ini,
3. Ibu Umi Fadlilah, S.T, M.Eng selaku Sekretari Praktek Prodi Jurusan Informatika Universtas Muhammadiyah Surakarta yang telah membantu peneliti dalam menyelesaikan laporan Kerja Praktek sebelumnya,
4. Bapak Fatah Yasin Irsyadi, S.T, M.T selaku Koordinator Kerja Praktek Prodi Jurusan Informatika Universtas Muhammadiyah Surakarta yang telah menjadi dosen pengajar,
5. Bapak Muhammad Kusban, S.T, M.T selaku dosen dan pembimbing skripsi peneliti yang telah membimbing peneliti sehingga skripsi dapat

terselesaikan,

6. Dosen - dosen FKI Prodi Informatika yang telah mengajar dan memberikan pengetahuan kepada peneliti selama menempuh proses perkuliahan,
7. Adjie Sapoetra, S.Kom selaku Koordinator Skripsi Prodi Informatika Fakultas Teknik Informatika yang selalu memberikan informasi berkaitan dengan proses pembuatan skripsi,
8. Kedua orang tua yang selalu mendukung peneliti untuk menyelesaikan skripsi ini dengan baik,
9. Teman - teman FKI angkatan 2011.

Sekali lagi peneliti mengucapkan terimakasih kepada beliau - beliau beserta teman - teman yang tentunya tidak dapat peneliti sebutkan satu persatu.

Surakarta, 24 Juli 2015

Alim Nuryanto

L200110022

ABSTRAK

Server merupakan perangkat yang telah ter-integrasi dengan spesifikasi *hardware* tertentu, dan *software* yang memiliki fungsi tertentu seperti ftp, ssh, web server. Layanan tersebut rentan akan serangan yang dapat menimbulkan kerugian. Oleh karena itu diperlukan sistem pendukung yang mampu mendeteksi sebuah aktifitas jaringan. Suricata adalah IDS yang mambu mendeteksi sebuah aktifitas jaringan dan mengidentifikasi ancaman serangan dibantu dengan *rules* yang ter-intergasi. Suricata memindai setiap datagram yang dikirim pada sesi TCP dan mengubah menjadi informasi dan dikirim pada pada aplikasi Snorby untuk diolah. *Rules* pada suricata berperan dalam mengidentifikasi serangan yang terjadi pada sebuah host.

Kata kunci : Server, *Suricata, Snorby, Rules, IDS,*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR SINGKATAN

ACK : *Acknowledgment*

Csum : Cheksum

Dst. Port : *Destination Port*

HLEN : *Header Length*

ID : *Identifier*

IDS : *Information Detection System*

Len : *Total Length*

Off : Data Offset

Offset : Fragment Offset

Proto : Protokol

Seq : Sequence

Src. Port : *Source Port*

TOS : *Type Of Service*

TTL : *Time To Live*

URP : *Urgent Pointer*

Ver : Versi

Win : *Window*